HOW DEVICE-BASED GEO-FENCING WORKS TO IMPROVE EMERGENCY ALERT ACCURACY

WHITE PAPER

ONE2MANY

AN EVERBRIDGE COMPANY

INTRODUCTION

At the heart of public warning is the ability to reach the at-risk population about an imminent threat, in a timely manner. Studies have shown that effective early warning not only saves lives but minimizes damage to property and infrastructure. How do you inform the right people, at the right time, in the right place?

The ever-present mobile device is, globally, the best go-to option. It just makes sense. A mobile device is at your side almost 24*7. Sending alerts to the mobile device lets Government agencies reach the largest amount of the population and communicate relevant guidance to safety.

The Government alert originators have the task of deciding the radius of the alert: which mobile devices to target. Setting the target area too wide may cause unnecessary confusion which could impede the emergency service's efforts. Conversely, set the area too small and there's a risk of casualties and, or damage. Yet, it's up to the Mobile Network Operator (MNO) to turn the requested target area into reality. After all, it's the mobile network which delivers the emergency alerts to the user.

In this white paper, we look at

- The evolution of emergency alert targeting
- A deeper dive into device-based geo-fencing
- Some limitations and impacts to bear in mind

THE EVOLUTION OF EMERGENCY ALERT TARGETING

From wildfires and floods to riots and uprisings, as well as the COVID-19 pandemic, 2020 highlighted the pivotal role public warning solutions play in keeping people safe. Communicating swiftly to the right people at the right time, with the right information makes all the difference.

Effective public warning requires the Government and the Mobile Network Operators (MNOs) to work in harmony. With the MNOs' infrastructure being the backbone for the alert dissemination. How does it work? Using their public warning portal, alert originators define the target area for the emergency alert with the associated guidance to safety. It's here that the baton is handed over to the MNO. They are responsible for delivering the targeted alerts. So, how does the target area from the portal get mapped onto the mobile telecoms network and reach the relevant mobile device?

Let's use the Wireless Emergency Alert (WEA) system to explain.

The Warning, Alert & Response Network (WARN) act established WEA in 2008. WEA is a public/private partnership between the Federal Communications Commission (FCC), Federal Emergency Management Agency (FEMA) and the wireless industry to enhance public safety. WEA focuses on geographically targeted alerts using Cell Broadcast.

For over a decade, it's fallen to the Alliance for Telecommunications Industry Solution (ATIS) to convert the various FCC WEA mandates to an implementable WEA system. one2many's Peter Sanders is an active member of ATIS and contributes to the ATIS Wireless Technologies & Systems Committee (WTSC) that plays a vital role in defining the WEA standards. Although ATIS is the North American standards body, WEA isn't applicable to only there. As part of 3GPP, the ATIS WEA standards for Cell Broadcast have been validated for use globally.

WEA 1.0

Initially WEA 1.0, based on FCC Report and Order 08-99A1 and 08-164A1, indicated the target area by a mandatory geocode. What does this mean? In practice, it's using geo-targeting on a county level. In WEA 1.0, the use of the radio network's polygons and circles were optional. In hindsight, ATIS specification J-STD-101 was ambiguous. This ambiguity meant vendors could ignore the polygons and circles in their solutions if they chose to, focusing solely on the union of the geocodes. However, it became clear that those geocodes were too far reaching, often leading to over-alerting, especially in big counties. For instance, people in the valley and those living on the hillside received the same guidance to safety.

WEA 2.0

To increase the accuracy, WEA 2.0, associated with FCC Report and Order 16-127, enhanced the geo-targeting requirements with the cell selection being based on polygons and circles. This version saw the original radio network polygon being retrieved, enabling the Cell Broadcast Center (CBC) to map the alert originator's area onto the cell sectors within the polygon. As is common with standards, to maintain backwards compatibility, the geocode was still mandatory within WEA 2.0.

Although an improvement, the FCC had the ambition to provide even more granular accuracy. Their goal was to provide targeted guidance to 100% of the people inside the target area, with no more than 0.1 miles (160 meters) overshoot. What does that look like? It equates to sending alerts to only people on a specific city block.

WEA 3.0

In both WEA 1.0 and WEA 2.0, all devices that were in the coverage area of the addressed cells received and were presented with the public warning alert from the CBC. Even those devices that were outside of the alert originator's target area, as drawn in their public warning portal's dynamic mapping functionality. The latter happens if, for instance, the target area is in part of the addressed cell's coverage area.

It was FCC Report and Order 18-04 of January 2018, that defined the mandate to improve the geo-targeting accuracy to 100% of the population by November 2019. To prevent over-alerting from the CBC cell selection, the outcome of WTSC's work was the introduction of a device-based geo-fencing (DBGF) capability, referred to as WEA 3.0. This new capability applies to 4G and 5G networks.

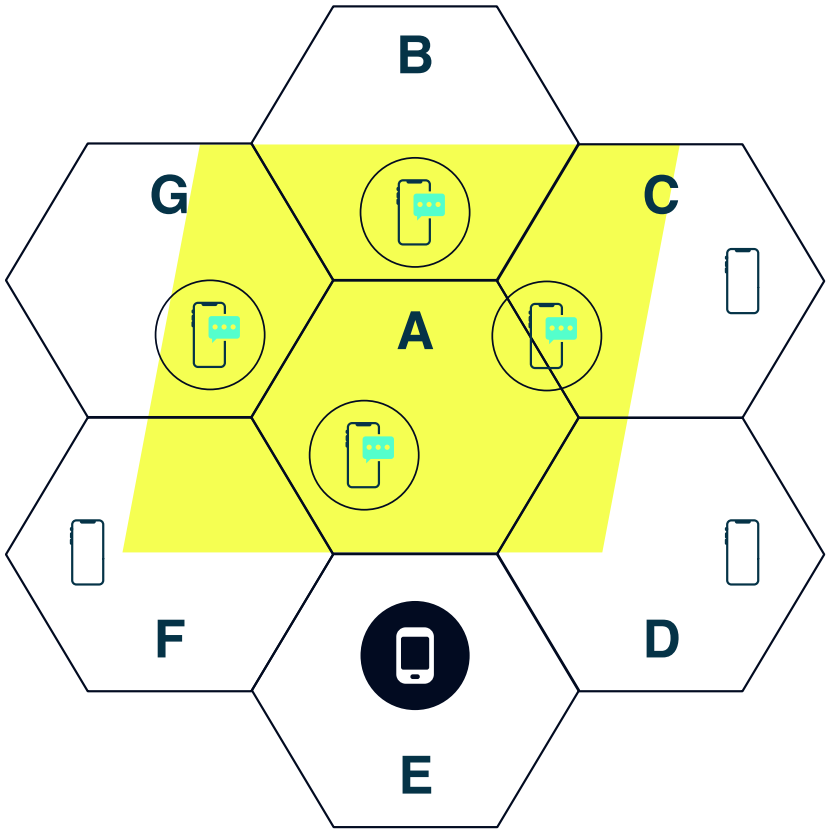
In layman's terms, with WEA 3.0, reliance now falls onto the mobile device's location technology (for example, GPS, Wi-Fi, Bluetooth, etc.) to determine whether it is located inside or outside the target area. What role does DBGF play? DBGF controls if the public warning alert is presented to the user. However, due to the standards requirement of 100% reach within 0.1 miles (160 meters), the underlying MNO policy for geo-targeting is more likely to favor over-alerting versus optimal- or under-alerting.

In reality, the mobile device's capability to geo-locate itself, is in the realms of meter accuracy. It's part of what helps us arrive at our destination when using Google Maps, Garmin or TomTom navigation systems, for instance.

How does DBGF work in practice?

The alert originator defines the target area by drawing polygons and circles on their dynamic map in their public warning system (PWS). The polygon, in this example below, is the yellow shaded area on the diagram below. The target area is then passed over to MNO domain, where the CBC selects the appropriate cells that cover the specified target area, based on the MNO policy. With WEA 3.0, the network includes the target area geometries (polygons and circles) in the Cell Broadcast (CB) message itself. WEA 3.0 compatible mobile devices use their location technology to determine if the device is located inside or outside the target area with a meter's accuracy. If the device is inside the area or the device can't determine its location, the device will display the emergency alert to the user. As this capability is standards-based, it means that it's backward compatible. Mobile devices that support WEA 1.0 and WEA 2.0 will work as before.

The results look like this.



The yellow shading (the polygon) is the target area defined by the alert originator. It includes cell sites A, B, C, D, F and G. But the polygon doesn't include cell site E. Based on the target area, the identified cell sites will broadcast the alert for this geometric shape. All mobile devices in those target sites will receive the alert.

Now let's add the DBGF dimension to the picture. For a network **without** DBGF, all devices in target cells will receive the alert. In a network **with** DBGF, **only** the mobiles with the green message symbol, that are located inside the polygon, will present the alert. The mobile in the black circle will not present any alert, as it's located in cell site E, which was not part of the alert originator's target area. The CBC continually broadcasts the guidance to safety message. If new mobile devices enter the target area, the alert will be presented. Devices which have already presented the specific alert will not present it again.

A DEEPER DIVE INTO DEVICE-BASED GEO-FENCING

Now we have established the basic concept of DBGF, let's look at what this means on a more technical level by delving into different aspects.

- **How does a mobile device know where it is?**

It is the Operating System (OS) of the mobile device that enables the device to geo-locate itself. It is a proprietary procedure. As no standard exist that specifies this, we can assume that for the determination of the location, the mobile device uses multiple sources, for instance GPS, Wi-Fi, Bluetooth, etc. For European Member States, the 12 December 2018, Commission Delegated Regulation (EU) 2019/320 requires that at least Galileo and Wi-Fi are used to determine location of devices that access emergency services. For Wi-Fi, the mobile device obtains the Service Set Identifiers (SSIDs) that it can receive and requests a Google server for the locations of those Wi-Fi networks.

Despite how useful this is in practice; will this proprietary procedure ever be standardized? The European Commission has sent a Standardization Request to ETSI to develop, among others, a standard for exactly this. However, some ETSI members have objected, so ETSI has rejected the mandate. The Commission hasn't given up. More may follow.

Getting the polygon to the phone

In addition to the target area geometries as specified in 3GPP TS 23.041 (version 15.40 and later), a new element was included – *WarningAreaCoordinates*. These coordinates are added to the *Write-Replace-Warning* Request which the CBC sends to the Radio Access Network (RAN) for broadcasting. They contain the polygons and circles as specified by the alert originator. Why is that important?

By sharing the *WarningAreaCoordinates* - the target area is included in the CB message, itself. The coordinates help the mobile device determine if it's in the target area or not.

After the mobile device, that supports WEA 3.0, receives the first CBC message with the *WarningAreaCoordinates* elements included, it will perform the geo-fencing procedure. What do we mean by that? If the mobile device determines its own location is inside the defined target area, the CB message is presented to the user. However, if the mobile device determines that it is outside of the target area, then the device stores the message. The message is not presented to the user. What happens if the *WarningAreaCoordinates* element is not included in the message? The mobile device will present the CB message to the user regardless of its location. As you can see, the mobile device now plays an active role in the end-to-end delivery of a CB public warning alert.

How are repeated messages handled?

Traditionally, CB messages are repeated, but when such a repeated message is received it is discarded at the modem layer. Why? The modem layer has already passed on this message once before to the upper layer, where the geo-fencing procedure is done. In practice, this means the stored message is never rechecked for its location. With WEA 3.0, the network broadcasts geo-fencing trigger messages.

The geo-fencing trigger message is a CB message with Message Identifier 4400. The CB message contains, in its payload, the Serial Numbers and Message Identifiers of the messages that require a re-check of the location. If the mobile device is inside the area that was included in a stored message, or if the device cannot determine its location, then the stored, and triggered message will be presented. If the mobile device determines it is still outside the area, nothing will happen. The CB message is not presented to the user.

Once a mobile device has received a geo-fencing trigger message any subsequent rebroadcasts of that trigger message are discarded at the modem layer as duplicates. What happens when the mobile device shall perform another geo-fencing procedure for stored messages? The network broadcasts a geo-fencing trigger message with a new Serial Number. Since that message is new for the mobile device it will be passed to the upper layer to trigger the geo-fencing procedure.

What's the difference between the upper layer vs modem layer in a mobile device?

A CB message is received at the modem layer. Even though 3GPP specifications specify that checks are performed at the upper layer, in reality, the check for duplicates happens at the modem layer. What is a duplicate message? It's a message that is received within 24 hours with the same Serial Number and Message Identifier as a message that was previously received and passed to the upper layer.

The upper layer consists of the OS (e.g. Android or iOS) and the native applications. A native application is not a downloadable application but is part of the OS. However, such an application is added by the Device Manufacturers, such as Samsung, Huawei, and Apple, and not by the supplier of the OS. In the case of Google, from Android 11 onwards, the public warning system client is included so there's no longer a need for the Device Manufacturer to provide this client.

LIMITATIONS AND IMPACT

Given the criticality of public warning, it's essential that every alert reaches the targeted mobile device. Along the way, there are different factors which can influence the accuracy and receipt of that alert. What's involved in presenting an alert to a user? Let's break it down.

The mobile device itself has multiple filters that determines whether an alert should be presented. One of those filters is the severity level. A mobile device determines if alerts should be presented based on Settings. For instance, has the user opted out of receiving particular alerts?

The same concept applies for DBGF. It's another filter that the mobile device uses to determine if the message is presented: is the user's mobile device within the target area or not. What happens if there is an occasion where there are two guidance to safety messages active in the same cell? For example, in rural areas the cell coverage areas can be very large, sometimes 30 kilometers in diameter. With DBGF it is possible to address only the people that need to be alerted in that segment of the large rural cell.

Yet, for the alert to be presented on the right device, at the right time, there are a number of limitations that have to be taken into account. Although not an exhaustive list, here are few to bear in mind.

Polygons

The polygon that is included in the CB message contains a maximum of 100 coordinate pairs. This can be handled in the alert originator's front-end system, their Cell Broadcast Entity (CBE). For example, let's take a one2many CBE. The Public Warning Platform automatically ensures when the alert originator is using the DBGF indicator that the number of polygons and circles used in the alert is not more than 10 or the total number of coordinate points is not more than 100, when sending an alert to the CBC. However, not all CBEs perform this automatically.

GPS interference or scrambling

The accuracy of the GPS and the ability of the device to geo-locate itself changes over time. Why does this matter? Often it gets better, but there are times where it gets worse either induced or resulting from environmental effects. This means that the mobile device's algorithms have to find more data points, not only from GNSS, such as GPS but also from cell sectors, Wi-Fi, and the wireless network. All these data points combined improve the mobile device's ability to geo-locate itself. Although these algorithms are within the realm of the Device Manufacturer they need to be taken into account when it comes to the delivery accuracy of the alert.

Mobile devices that can't geo-locate themselves

There is never a time where all the users have the latest mobile device. Naturally, there is always a mix of device capabilities within the network. How does an MNO handle alerting to those devices which can't geo-locate themselves? In truth, the MNO doesn't need to handle it. It's done by the mobile device. Where a mobile device can't geo-locate itself, or if the time-out setting is exceeded, the CB messages is delivered as it always has been. The general rule of thumb is, it's better to present the alert than not, even if the mobile device is not specifically within the alert originator's target area.

Device-based geo-fencing device support

Moving onto specific support for WEA 3.0. As we've seen, the mobile device plays an active role in WEA 3.0. That active role requires mobile devices that support WEA 3.0 DBGF.

As is the case for any new functionality, with WEA 3.0 only going live in the US in September 2019, there is a lag period before all Device Manufacturers to have incorporated and rolled out devices that support this capability. The good news is that most high-end devices support WEA 3.0, and that number will continue to increase over time. How can you find out the support device levels? Each MNO usually publishes the device support status.

When it comes to Android based devices, from Android 11 onwards they support the WEA application natively. This includes DBGF.

Network impact

It's not just mobile devices that need to support WEA 3.0, so too does the MNO's network. This requires an upgrade to the CBC to include the *WarningAreaCoordinates* element in the *Write-Replace-Warning-Request* message. From a CBC perspective, one2many's already fully supports WEA 3.0.

Then there is also the Evolved Packet System (EPS), the Mobile Management Entity (MME) needs to support that element and the eNodeB needs to include that element in SIB12 for broadcasting over E-UTRA. When it comes to 5G, the Access and Mobility Management Function (AMF) is not impacted. Why? The *Write-Replace-Warning-Request* passes transparently through the AMF. The gNodeB needs to include that element in SIB8 for broadcasting over New Radio (NR).

CONCLUSION

WEA 3.0 is, undoubtedly, a game-changer in the public warning world. With improved accuracy levels, alert originators are better able to provide specific and tailored guidance to safety messages. Yes, WEA 3.0 is only relevant for 4G and 5G networks and there are some upgrades required on the MNO side. But this is no different to other technology evolutions that MNOs have faced before. As with all new technology, there is a transition time to take into account, including network and device updates. The good news is, with WEA 3.0 being standards-based, the backwards compatibility ensures that public warning alerts can still be received, no matter what mobile device a user has.

How do you decide what's the best approach to be ready for WEA 3.0? Whether it's just advice or an upgraded solution, you can't go wrong working with a vendor who has both a proven track record in deploying and managing public warning solutions globally as well as being an active contributor to the industry standards bodies, like one2many.

INFO@ONE2MANY.EU

ONE2MANY

AN EVERBRIDGE COMPANY